Security Watch

A QUARTERLY PUBLICATION

CONTENTS

CASE STUDIES

ADVERTISER-SPONSORED

SECURITY WATCH NOVEMBER 2003

This special advertising section was produced by the *Windows & .NET Magazine* Custom Media Group in conjunction with Microsoft. This supplement appears as an insert in the November 2003 issue of *Windows & .NET Magazine*. For information about Custom Media opportunities, contact Don Knox (dknox@winnetmag.com).

Don't Wait:

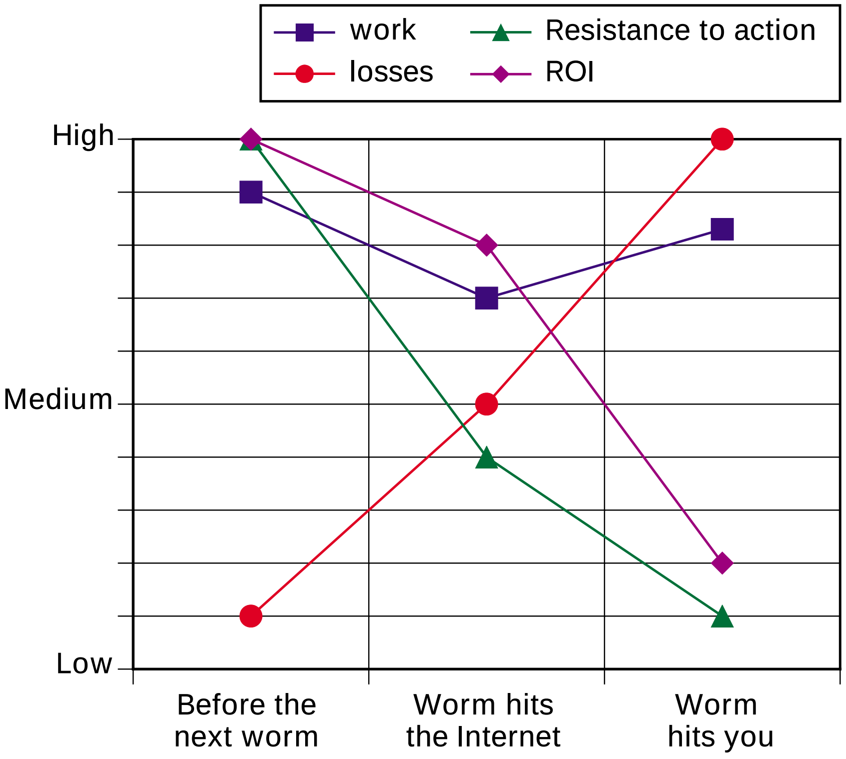
Prepare Your Network Now for the Next Attack

by Randy Franklin Smith

CodeRed came and went. Nimda struck. Then Blaster swarmed across the Internet. Like so many barbarian hordes, worm after worm descends on our networks, raping and pillaging as they go, interrupting commerce and diverting IT staff away from projects critical to business objectives. Again and again IT finds itself fighting hand-to-hand combat with malware in the streets of their network, poorly matched against an enemy that operates at Pentium speed and needs no sleep.

If the combined community of intranets and the Internet were a feudal civilization from long ago, historians would look at us in wonder. Though raided over and over again we fail to reinforce our gates. Though razed by burning arrows more than once, we don't replace our roofs of volatile straw with slate. Historians might be tempted to write us off as a people grown complacent from decades of relative peace and security before things were so connected and before writers of malware had such a ripe venue for their nihilistic urges.

But such would be a premature conclusion. Looking a little deeper one sees the challenges involved. It’s easy to say, “Keep your systems patched.” But how do you accomplish that when you have thousands of computers? Sometimes patches introduce new bugs. Where do you draw the line between stability and security? What about sales forces that remain disconnected from your network for weeks or months at a time. All it takes is one laptop to become infected, connect to your network, and unleash the swarm.



A lot of work is involved, but the earlier you respond to a worm, the greater the ROI

FIGURE 1: Risk Mitigation Factors and Their Relationships

START NOW TO MITIGATE RISK

While there’s no substitute for patching, there are ways to mitigate the risk and impact of the next worm. But mitigation requires a paradigm shift. Despite the fact that firewalls have been around a long time and their limitations have become well established, we still depend on them too much, leaving our networks like an egg—hard on the outside; soft and runny on the inside. To improve our situation, we must implement mitigating controls at three physical levels and understand three temporal stages where we have opportunities to mitigate either risk or impact. For instance, we tend to focus on protecting servers because they physically host the information and processes we need to protect, but insecure workstations have unwittingly served as springboards for malware to saturate networks. While there are many ways to address security risks, this article will describe these tertiary concepts and use IP Security Policies as a specific, example technology as a backdrop for demonstrating these concepts in practical terms.

Nowhere is the adage “an ounce of prevention is a worth a pound of cure” more apropos than in IT security. You have three chances to control and reduce the effects of the next worm. Figure 1 shows the inverse sliding scales of potential losses compared to the availability of management support for taking action. Note, however, that while the amount of work involved remains at a fairly static high, the ROI for the work diminishes as time goes on because the work shifts from strategic to tactical in nature. One security expert compares these three phases to stages of the economy. The first and best time to do something about the next worm is before it hits. We call this the expansion phase. When the economy is going well, orders are up, lines are running at full capacity and it’s hard to get people enthused about investments in cost cutting and efficiency. Likewise, it’s hard to muster resources and get management support to implement controls for threats that haven’t materialized.

Your next opportunity to mitigate risk is when the next worm becomes reality and shows up on the radar in security forums, but before it gets CNN’s attention. At this point, the worm has hit some of your neighbors but not you. We call this the recession phase—it’s late but you still have time to do something. Next, an unpatched server, a sales rep’s laptop or business partner’s computer brings the worm to your network, packet rates redline, and your support lines start ringing. Depression is in full swing but you can still reduce and control the losses if you keep your head and use the weapons at your disposal.

USING IP SECURITY POLICY

Windows 2000, Windows XP, and Windows Server 2003 all share a marvelous but underused technology called IP Security Policy. IP Security Policy, combined with Group Policy, is an incredibly powerful and flexible weapon that can be brought to bear on malware at each mitigation phase. Window's IP Security Policy is more than just an implementation of the IPSec standard. While normally viewed as a way to protect data on the network and prevent connections from untrusted hosts, IP Security Policies allow you to do much more. To protect against malware, you can use IP Security Policy to block packets based on IP address, port number, or failure to justify communication via a certain protocol.

Using IP Security Policy to mitigate risk during the expansion phase involves changing the nature of your network. If we were to compare packets to people, network cables to roads, and computers to towns, the normal corporate network would resemble a "free" country like the U.S. where people are allowed to travel widely and freely. But to mitigate the risk of the next worm, as well as intrusions by malicious agents in general, you must remodel your network to resemble a police state in which travel is highly controlled and is restricted to movement that is explicitly approved and that serves the interest of the state.

Additional Security Resources

Best Practices for Mitigating RPC and DCOM Vulnerabilities

http://www.microsoft.com/technet/security/virus/bpDCOM.asp

Security Guides

Windows Server 2003

Windows Server 2003 Security Guide
http://go.microsoft.com/fwlink/?LinkId=14845

Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP
http://go.microsoft.com/fwlink/?LinkId=15159

Windows 2000 Family

Windows 2000 Security Hardening Guide
http://www.microsoft.com/technet/security/prodtech/windows/win2khg.asp

Microsoft Solution for Securing Windows 2000 Server
http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp

Windows 2000 Common Criteria Evaluation
http://www.microsoft.com/technet/security/issues/w2kccwp.asp

Windows 2000 Common Criteria Security Configuration Guide
http://www.microsoft.com/technet/security/issues/W2kCCSCG/default.asp

Windows XP

Windows XP Security Guide

Download
http://go.microsoft.com/fwlink/?LinkId=14840

Online
http://go.microsoft.com/fwlink/?LinkId=14839

Patch Management

http://go.microsoft.com/fwlink/?LinkId=16284

Open Hack IV Hardening

http://msdn.microsoft.com/library/en-us/dnnetsec/html/openhack.asp

In technical terms, this means that you must analyze the traffic on your network with special attention to the various computer roles within your network and which applications and protocols are required by each. Then you create policies that limit traffic using the "least privilege" concept. Implementing a police state on your network provides a large dose of auto-immunity to yet-to-be discovered exploits and yet-to-be released worms. While the next worm may still be able to spread from infected computers to others through approved protocols and computer roles, it will spread much more slowly and the impact should be far less.

FIND WAYS TO CUT OFF THE NEXT WORM

But what if you don't have the resources or support to lock down your network ahead of time? Before a worm actually hits you, you have time to take tactical mitigation steps. Find out how the worm propagates and look for ways to cut it off or slow it down. For instance, Blaster exploited a weakness in RPC and spread through workstations—not just servers. In general, workstations don't need to accept incoming connections. But there are exceptions. Outlook clients, for example, receive new mail notifications from Exchange via RPC. But

how many Exchange servers are on your network? With Group Policy you can easily deploy an IP Security Policy to workstations that blocks incoming RPC locator traffic (TCP port 135) from all computers except Exchange servers. The quickest way to build such a policy is to define a filter for each Exchange server that looks for port 135 packets with the server's source address and lets them through.

Of course, filtering on source address can be impractical if you have many Exchange servers and it can be a maintenance task easily forgotten about when server IP addresses change or new severs are deployed. With a slightly greater investment in upfront work you can solve this problem by using IPSec's Authenticated Header (AH) mode. With IP Security Policy you can require a computer to authenticate with specific credentials before accepting packets from it. In this case, the object of using AH mode is not authentication itself but using authentication as a vehicle for authorization (i.e., identifying which computers are authorized to initiate connections via RPC).

Once a worm hits your network, your opportunity to mitigate the spread or impact is limited

The first step is to create a group called Exchange Servers and add the appropriate computer accounts as members. Next, create a group policy object (GPO) linked to the root of the domain. Edit the access control list (ACL) of the GPO so that only the Exchange Servers group has "Read" and "Apply group policy" permissions to that GPO. This step limits the GPO from being applied to any computers except for members of the Exchange Servers group. (If you already have an organizational unit that contains all your Exchange servers you could simply link the GPO to that OU and leave the ACL with its default permissions.)

Next, configure the GPO's IP Security Policy to use a specific encryption key when connecting to computers via port 135, if demanded by the computer. After the Exchange servers apply their new GPO, configure another GPO linked to your workstations that requires AH mode and the same encryption key for incoming connections to port 135. By deploying the proper credentials only to Exchange servers, they will be the only computers that can successfully connect via RPC to your workstations, which (except for a comparatively small number of Exchange servers) protects more than 95 percent of the computers in a typical network from infection by RPC-born malware.

TAKING ACTION AFTER A WORM HITS

Once a worm hits your network, your opportunity to mitigate the spread or impact is limited. Don't delay implementing your malware response plan while you're making last-ditch efforts to stop the worm. Instead, mitigation efforts should take place in parallel with your normal response plan with different staff. To mitigate the worm at this point, you need to assess what is known about the worm's propagation and LAN usage characteristics and analyze that information in relation to your network.

Look for a choke point where you can stop or slow down the spread. For instance, if you have centrally managed, deep layer switches perhaps you can push out a policy that blocks the worm based on a port number or packet content. If the worm uses a well-known protocol, determine which applications on your network use that protocol. Then deploy an IP Security Policy that blocks that protocol to any systems where the related applications are not needed or are non-critical. A more ham-fisted but effective approach used by one company was to instruct all their users to activate Internet Connection Firewall.

If the outbreak is quickly detected in one data center, try to contain it to that location through router policies. Such an attempt would require cooperation from multiple parties and an accurate grasp of what will break if a given type of traffic is severed between parts of your network, which brings us back to the value of advance preparation.

The earlier you start working to stop the next worm, the more you'll mitigate its effects and reap long-term benefits for your effort. Use the tools at your disposal now to shore up your defenses. Implement Software Update Services or Systems Management Server to deploy patches automatically. Lock down your network with IP Security Policies so that malicious packets have a difficult time making it around your network. Think about mitigating controls that you can implement deeper in your network than just at the perimeter, such as on the network itself at switches and computers—for both servers and workstations. You'll be a hero when the next worm gallops across the Internet and your network comes through unscathed. ◆

Randy Franklin Smith is a contributing editor for *Windows & .NET Magazine* and the primary instructor and course developer for MIS Training Institute's Windows NT/2000 security program. His firm, Monterey Technology Group, provides security consulting.

Smoothing the Path:

ISA Server VPN Deployment Kit Provides Step-by-Step Instructions

As you might be aware, the combination of Internet Security and Acceleration (ISA) Server 2000 and Routing and Remote Access Service (RRAS) provides an amazing number of possibilities for securing your perimeter's network while still allowing access to remote users or offices—and for publishing internal servers to the Internet. With ISA Server and RRAS, you can

- create site-to-site VPNs
- create remote access VPNs for traveling users or telecommuters
- publish Web, ftp, Exchange and other email servers using application-level gateway filtering
- leverage your Active Directory (AD) infrastructure and reduce identity management problems because there's no need to create additional firewall or VPN accounts for your users
- control remote access to network resources using groups defined in AD—even assigning packet filters and day and time restrictions to specified groups
- support clustering and other fault-tolerant and scalability options
- leverage the VPN client that is already present on your Windows clients instead of having to load additional client software
- set up high-security remote access VPNs that require dual authentication and function even across firewalls that use NAT, but still support all Windows clients from Windows 98 forward
- use quarantine technology to enforce security policies on any computer connecting to your network

In the past, however, all this rich functionality has been difficult to exploit because of a deluge of piecemeal documentation. Today, to help you get the most out of ISA Server and RRAS, Microsoft offers the ISA Server 2000 VPN Deployment Kit, which was developed by ISAserver.org (http://www.isaserver.org), an independent ISA Server resource site. Microsoft sponsored development of the VPN Deployment Kit as part of the company's Trustworthy Computing initiative. While ISAserver.org is not affiliated with Microsoft, the company recognizes that the organization has helped the success of ISA Server, and Microsoft often refers people seeking support to the organization's Web site.

TAKING A NEW APPROACH

Given the depth and breadth of ISA Server and RRAS's features, as well as the wide variety of network scenarios encountered at today's enterprise networks, you can easily become overwhelmed by the details. The VPN Deployment Kit takes a new approach to documentation designed to help you accomplish the specific goal you wish to reach with ISA Server. A modular, targeted approach helps you go directly to the information you need to set up ISA Server for your particular VPN scenario. You can bypass all the extraneous details and features that have no bearing on your situation.

The VPN Deployment Kit's 30 documents are tied together by a key document called "How to Use the ISA Server 2000 VPN Deployment Kit." The key document presents several paths that you can select from. These paths direct you to the information you need in the order you need it. For instance, you can select the ISA Server 2000 VPN Networking Decision Points section, which leads you through a series of questions about your current environment and the type of VPN that you want to set up. By answering the questions you identify important decision points and you identify the articles you should read regarding the VPN you're trying to configure.

If you already know what you need to set up and how to do it, you can use the guide as a pre-flight check, reviewing each of the steps and considerations to make sure you don't miss anything when you make the actual changes in your production environment. Or perhaps you have a conceptual understanding of all the pieces you need to assemble, but you need step-by-step assistance for certain portions of your setup. You can scan the kit

for the relevant documents and brush up on the pertinent topics. No matter how you use the VPN Deployment Kit, in each document you'll find precise, step-by-step instructions accompanied by screen shots (more than 600 in all) that document nearly every step in the process being explained. You'll also find diagrams to help you grasp the concepts involved in each VPN scenario.

In each document you'll find precise, step-by-step instructions accompanied by screen shots

TAKING IT A SECTION AT A TIME

The first section in the kit, *VPN Deployment Guide Concept Documents*, provides two documents—"VPN Network Design Concepts—Overview of VPN Networking Designs for Small and Medium Sized Business" and "Applying the ISA Server 2000 VPN Deployment Kit to VPN Network Scenarios—Using the VPN Deployment Kit Documents that Apply to your Network Design"—that will give you a solid understanding of ISA Server VPN concepts. The *VPN Server Configuration Documents* section provides instructions on fundamental procedures like "Installing and Configuring ISA Server 2000 on Windows Server 2003" and setting up Certificate Services on Standalone Certification Authorities (CAs) and Enterprise CAs to support L2TP. But the VPN Deployment Kit also handles more advanced topics, such as specific steps for deploying certificates manually and through Group Policy's auto-enrollment feature. Other documents in the VPN server section explain how to configure RRAS and your Internet Authentication Server to implement certificate-based user authentication using Internet Authentication Service and EAP-TLS and how to handle DNS name resolution and DHCP address assignment issues.

The *VPN Client Configuration Documents* section addresses issues surrounding the setup and support of Windows VPN clients. While all documents in the kit assume that you're installing ISA Server 2000 on a Windows Server 2003 server, the kit provides separate documents for each type of Windows VPN client, including Windows 98, 98SE, ME, NT, 2000, XP, and 2003. Other VPN Client Configuration documents include guidance for installing the Microsoft L2TP/IPSec VPN Client, which gives Windows VPN clients from Windows 98 forward the ability to use L2TP in place of the weaker PPTP. Another important feature of the Microsoft L2TP/IPSec VPN Client provides Network Address Translation Traversal (NAT-T) support so that you can VPN to your Windows 20003 VPN server via L2TP even when you're behind your home firewall or the firewall of another company that you're visiting.

Configuring firewalls to allow in-bound and outbound L2TP can be difficult, but step-by-step guidance is provided in "Configuring the ISA Server Firewall/VPN Server to Support LTP/IPSec NAT Traversal Client Connections" and in "Configuring the ISA Firewall/VPN Server to Support Outbound L2TP/IPSec NAT-T Connections." The client section also includes help for configuring network browsing correctly, preventing compromise to your network via a risk called "split-tunneling," and using Windows Server 2003's Connection Manager Administration Kit (CMAK) to automatically deploy dial-up connections for users instead of relying on them to manually configure them. Other sections in the VPN Deployment Kit include VPN gateway configuration documents, VPN failover and fault tolerance documents, VPN in DMZ environment documents, and VPN infrastructure documents.

THE KIT DRAWS FROM EXPERIENCE

The VPN Deployment Kit is not a collection of ivory tower, theoretical white papers. Instead, the kit draws from the experiences of thousands of ISA Server users. Dr. Thomas Shinder, the author of the VPN Deployment Kit and the moderator of ISAserver .org, is a recognized expert on ISA Server and VPNs. Through ISAserver .org, Dr. Shinder has facilitated the answers to more than 40,000 questions from ISA Server users experiencing real-life problems. Drawing upon that perspective, Dr. Shinder let the ISA Server community's needs and experience drive the content of the VPN Deployment Kit.

In cooperation with Microsoft, Dr. Shinder structured the kit to give you the most value in the least amount of time. The VPN Deployment Kit isn't a static work. Unlike typical documentation, the VPN Deployment Kit was released first in beta form and 100 participants helped refine the kit. In another departure from classic documentation, the VPN Deployment Kit is actively supported and kept up to date by Dr. Shinder and other members at ISAserver.org.

If you have a question regarding one of the steps in a scenario or if you encounter a problem not covered in the VPN Deployment Kit's documents, you can submit your question to ISAserver.org and get a quick answer. With ISA Server and the Windows Server System you get much more than a basic firewall and an OS. ISA Server and Windows give you the flexibility, security, availability, and scalability you need to handle every type of network situation. The ISA Server 2000 VPN Deployment Kit (available only at http://www.isaserver .org) helps you exploit all the capability that you've already licensed. ◆

The Security Readiness Kit Helps You Find Solutions Easily

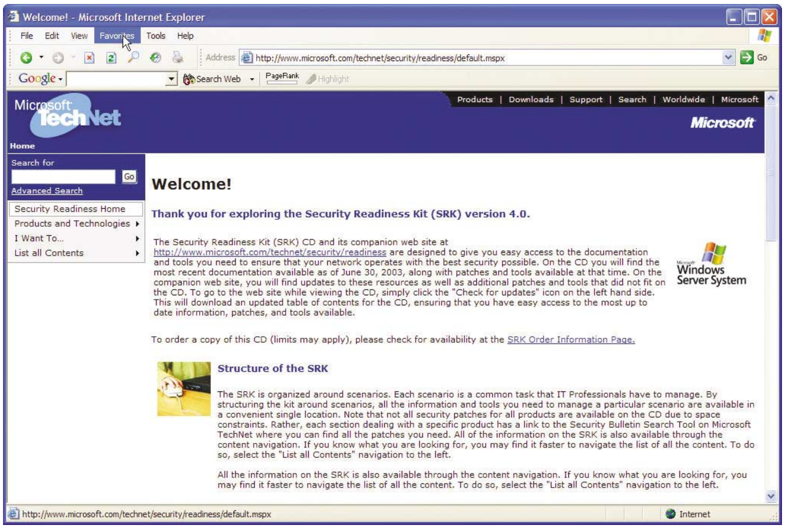
Keeping systems secure depends on effort from all of us. Microsoft leads the way by providing tools, guidance documentation, and other resources to help customers get secure and stay secure. A large part of getting and staying secure requires keeping systems up to date with the latest patches, and Microsoft provides multiple channels for patch information and deployment to fit the needs of everyone from consumers to large enterprises. These channels include Windows Update, Software Update Services (SUS), Systems Management Server (SMS), and the Security Readiness Kit (SRK) 4.0. Except for SMS Microsoft provides all these technologies at no charge.

Consumers and small businesses can use Windows Update (http://www.windowsupdate.com) to keep their systems patched without help from IT professionals. Medium-sized organizations can use SUS (http://www.microsoft.com/windows2000/windowsupdate/sus/) to deploy patches to thousands of systems automatically while being centrally controlled by an administrator. SMS (http://www.microsoft.com/smserver/default.asp) provides large organizations the maximum flexibility and power for managing tens of thousands of computers. The SRK (previously named "Security Resource Kit"), a different type of tool from Microsoft, is aimed at making sure customers have access to important security information and patches in as many ways as possible. The SRK is a library of service packs, tools and guides that you can access online or carry with you as a CD. You can access the SRK or order it on CD at http://www.microsoft.com/technet/security/readiness (see Figure 1).

GETTING A HANDLE ON PATCH MANAGEMENT

The SRK, which contains nine different guides to help ease the pain of implementing security processes within your network (e.g., patch management and perimeter security), can help you get a handle on patch management and other critical security processes. And because backing from management is crucial to the success of any security project, the SRK also contains information that will help you convey to management the importance of security processes such as regular patch deployment.

With the huge number of product versions, updates, and documentation available determining which updates need to be installed and which documents apply to your situation can be difficult. To tackle this challenge, Microsoft organized the SRK around scenarios. Each scenario listed under "I want to..." in Figure 2 corresponds to a common security task that IT professionals face regularly. For instance, some of the


Welcome! - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Address
http://www.microsoft.com/technet/security/readiness/default.mspx
Go
Google
Search Web
PageRank
Highlight
Products | Downloads | Support | Search | Worldwide | Microsoft
Microsoft TechNet
Microsoft
Home
Search for
Go
Advanced Search
Security Readiness Home
Products and Technologies
I Want To...
List all Contents
Windows Server System
http://www.microsoft.com/technet/security/readiness/default.mspx
Internet

Welcome!

Thank you for exploring the Security Readiness Kit (SRK) version 4.0.

The Security Readiness Kit (SRK) CD and its companion web site at http://www.microsoft.com/technet/security/readiness are designed to give you easy access to the documentation and tools you need to ensure that your network operates with the best security possible. On the CD you will find the most recent documentation available as of June 30, 2003, along with patches and tools available at that time. On the companion web site, you will find updates to these resources as well as additional patches and tools that did not fit on the CD. To go to the web site while viewing the CD, simply click the "Check for updates" icon on the left hand side. This will download an updated table of contents for the CD, ensuring that you have easy access to the most up to date information, patches, and tools available.

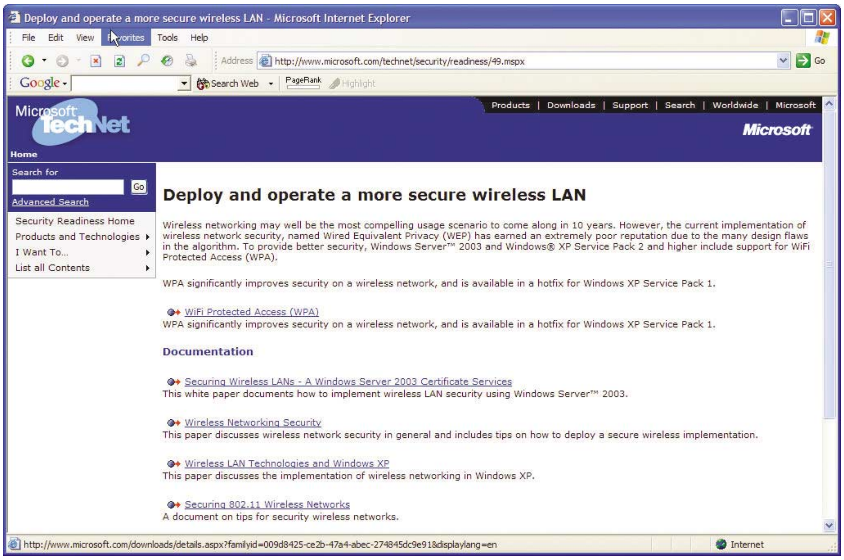
To order a copy of this CD (limits may apply), please check for availability at the SRK Order Information Page.

Structure of the SRK

The SRK is organized around scenarios. Each scenario is a common task that IT Professionals have to manage. By structuring the kit around scenarios, all the information and tools you need to manage a particular scenario are available in a convenient single location. Note that not all security patches for all products are available on the CD due to space constraints. Rather, each section dealing with a specific product has a link to the Security Bulletin Search Tool on Microsoft TechNet where you can find all the patches you need. All of the information on the SRK is also available through the content navigation. If you know what you are looking for, you may find it faster to navigate the list of all the content. To do so, select the "List all Contents" navigation to the left.

All the information on the SRK is also available through the content navigation. If you know what you are looking for, you may find it faster to navigate the list of all the content. To do so, select the "List all Contents" navigation to the left.

FIGURE 1: The Security Readiness Kit home page



Deploy and operate a more secure wireless LAN - Microsoft Internet Explorer

http://www.microsoft.com/technet/security/readiness/49.mspx

Deploy and operate a more secure wireless LAN

Wireless networking may well be the most compelling usage scenario to come along in 10 years. However, the current implementation of wireless network security, named Wired Equivalent Privacy (WEP) has earned an extremely poor reputation due to the many design flaws in the algorithm. To provide better security, Windows Server™ 2003 and Windows® XP Service Pack 2 and higher include support for WiFi Protected Access (WPA).

WPA significantly improves security on a wireless network, and is available in a hotfix for Windows XP Service Pack 1.

WiFi Protected Access (WPA)
WPA significantly improves security on a wireless network, and is available in a hotfix for Windows XP Service Pack 1.

Documentation

Securing Wireless LANs - A Windows Server 2003 Certificate Services
This white paper documents how to implement wireless LAN security using Windows Server™ 2003.

Wireless Networking Security
This paper discusses wireless network security in general and includes tips on how to deploy a secure wireless implementation.

Wireless LAN Technologies and Windows XP
This paper discusses the implementation of wireless networking in Windows XP.

Securing 802.11 Wireless Networks
A document on tips for security wireless networks.

http://www.microsoft.com/downloads/details.aspx?familyid=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

FIGURE 2: A scenario-based path to solutions

scenarios covered are “Deploy and operate a more secure Exchange environment including Outlook Web Access,” “Deploy and operate a more secure wireless LAN,” and “Find and deploy the latest software updates across my network.”

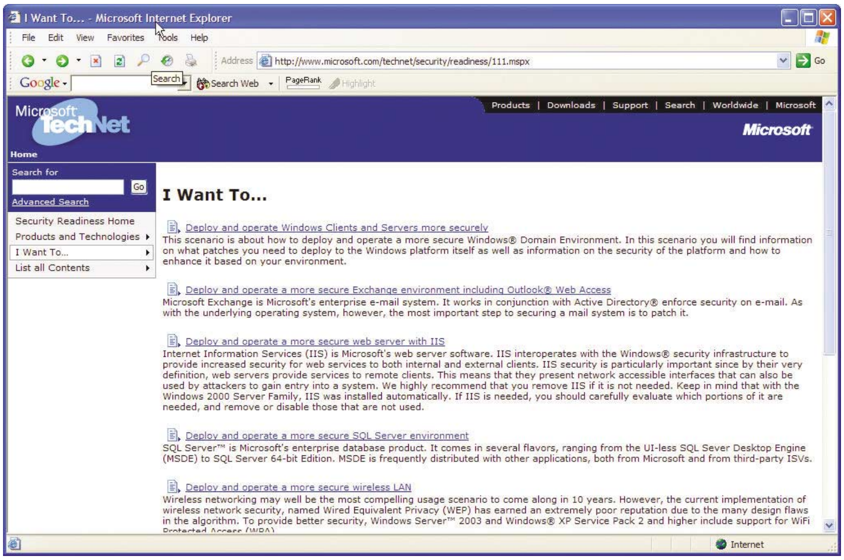
When you drill down into a scenario, the SRK explains the required products and versions and provides the appropriate updates and documents to help you reach your goal. For instance, in Figure 3, the “Deploy and operate a more secure wireless LAN” scenario explains the problems with Wired Equivalent Privacy (WEP), how WiFi Protected Access (WPA) solves them, and that you need Windows Server 2003, Windows XP Service Pack 2, or the “Windows XP Support Patch for Wireless Protected Access” (a hotfix for Windows XP Service Pack 1). In addition, the SRK provides five documents about wireless security: “Securing Wireless LANs—A Windows Server 2003 Certificate Services,” “Wireless Networking Security,” “Wireless LAN Technologies and Windows XP,” “Securing 802.11 Wireless Networks,” “Mobility: Empowering People through Wireless Networks,” and “5-Minute Security Advisor—Deploying 802.1X with Windows XP.” If you already know the subject you’re looking for, you don’t have to access it through the scenario path. Instead, you can go right to the subject by using the “List all Contents” navigation as shown in Figure 1.

PROVIDING OFFLINE ACCESS TO SECURITY TOOLS

Being able to access service packs and tools without connecting to the Internet is very important when setting up new systems. Sometimes, newly installed systems are hacked before the administrator has a chance to patch and harden the system. With the SRK you can load security fixes before ever connecting the system to a network. The SRK provides security guides, service packs and links to updates for all supported OSes and major server applications, including Windows Server 2003, Windows 2000, Windows XP, Windows NT, Exchange Server, Internet Information Server (IIS), Internet Security and Authentication (ISA) Server, SMS, and SQL Server (including the desktop version of SQL Server—Microsoft Data Engine. Because many of these materials are updated regularly the SRK CD links you to appropriate pages on the Microsoft TechNet Web site so that you can obtain the most up-to-date information.

Part of staying secure is making sure the software you are running is still supported and it’s important to understand that installing the next-most recent service pack and all the patches may not bring you to the same level of security as applying the most recent service pack and all its patches. Microsoft supports major product releases for up to seven years after release. In addition, Microsoft supports at least the most recently released version of the product and the version prior to that. Within products, Microsoft supports the most recently released service pack and, if the most recent service pack is less than a year old, the next most recent service pack is also supported. If there are fewer than two service packs released for a product, the most recent service pack and the original product release are both supported. See http://www.microsoft.com/windows/lifecycle/ for more information about the Windows Life Cycle. Hence, security updates are no longer available for MS DOS, Windows 3.xx, Windows 95, Windows NT 3.5x, Windows 98 / 98 SE, Windows Millennium Edition, and Windows NT Workstation 4.xx. As an exception to policy Microsoft plans to provide security updates for

The SRK provides security guides, service packs and links to updates for all supported OSes and major server applications


I Want To... - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.microsoft.com/technet/security/readiness/111.mspx
Go
Google
Search
Search Web
PageRank
Highlight
Microsoft TechNet
Products | Downloads | Support | Search | Worldwide | Microsoft
Microsoft
Home
Search for
Go
Advanced Search
Security Readiness Home
Products and Technologies
I Want To...
List all Contents
Internet

I Want To...

Deploy and operate Windows Clients and Servers more securely

This scenario is about how to deploy and operate a more secure Windows® Domain Environment. In this scenario you will find information on what patches you need to deploy to the Windows platform itself as well as information on the security of the platform and how to enhance it based on your environment.

Deploy and operate a more secure Exchange environment including Outlook® Web Access

Microsoft Exchange is Microsoft's enterprise e-mail system. It works in conjunction with Active Directory® enforce security on e-mail. As with the underlying operating system, however, the most important step to securing a mail system is to patch it.

Deploy and operate a more secure web server with IIS

Internet Information Services (IIS) is Microsoft's web server software. IIS interoperates with the Windows® security infrastructure to provide increased security for web services to both internal and external clients. IIS security is particularly important since by their very definition, web servers provide services to remote clients. This means that they present network accessible interfaces that can also be used by attackers to gain entry into a system. We highly recommend that you remove IIS if it is not needed. Keep in mind that with the Windows 2000 Server Family, IIS was installed automatically. If IIS is needed, you should carefully evaluate which portions of it are needed, and remove or disable those that are not used.

Deploy and operate a more secure SQL Server environment

SQL Server™ is Microsoft's enterprise database product. It comes in several flavors, ranging from the UI-less SQL Sever Desktop Engine (MSDE) to SQL Server 64-bit Edition. MSDE is frequently distributed with other applications, both from Microsoft and from third-party ISVs.

Deploy and operate a more secure wireless LAN

Wireless networking may well be the most compelling usage scenario to come along in 10 years. However, the current implementation of wireless network security, named Wired Equivalent Privacy (WEP) has earned an extremely poor reputation due to the many design flaws in the algorithm. To provide better security, Windows Server™ 2003 and Windows® XP Service Pack 2 and higher include support for WiFi Protected Access (WPA)

FIGURE 3: A sample “I Want To...” path

Windows NT Server 4.0 until January 1, 2005. If, as part of Windows NT 4.0, you use IIS 4.0 don't forget that IIS requires Internet Explorer. Because Internet Explorer 5.5 SP2 support expires on December 31, 2003, you should update IIS 4.0 servers to at least IE 6.0 SP1, which is included on the SRK.

The SRK contains the most recent service pack for Microsoft's major products, as well as links to the next-most recent supported service pack, if there is one. In addition, you'll find links to all the critical patches for the most recent service pack, as well as links to the critical patches for the next-most recent service pack. The service packs you'll find on the SRK are Windows NT 4.0 Service Pack 6A, Internet Explorer 6 SP1, Windows 2000 Service Pack 4, Windows XP Pro Service Pack 1a, Exchange 2000 Service Pack 3, Exchange Server 5.5 Service Pack 4, SQL Server 7.0 Service Pack 4, SQL Server 2000 Service Pack 3a, MSDE 2000 Service Pack 3, and ISA Server 2000 Service Pack 1.

THE SRK STAYS CURRENT

The SRK includes Microsoft's security tools, including Microsoft Baseline Security Analyzer (MBSA) 1.1.1, SUS 1.0, SMS Feature Pack, and Group Policy Management Console (GPMC). You can use MBSA to scan your entire network, including Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003 computers for common security misconfigurations, as well as for missing security updates. MBSA security misconfiguration scanning includes searching for vulnerabilities in Windows, Internet Explorer, passwords, IIS, SQL, and MSDE. The SMS Feature Pack is an add-on for SMS 2.0 that Microsoft designed to help administrators manage patches on large enterprise networks. The Feature Pack lets you package and install security patches to SMS clients automatically by using SMS's normal package deployment feature. The SMS Feature Pack regularly obtains a listing of newly released updates from the same data source that drives SUS. The GPMC provides a much advanced user interface for managing group policy objects (GPOs) in your Active Directory domain which helps you define, test and diagnose centralized security policies that you define in GPOs.

More than ever having a patch management process in place is crucial. Regular installation of patches is the only way to defend against some risks today. The SRK is designed to help you stay on top of the constantly changing security landscape. Because security patches, service packs, guides, and tools are updated regularly, Microsoft designed the SRK to automatically update itself. To download an updated table of contents for the SRK, just click the “Check for updates” icon on the left-hand side of the SRK CD's home page. It's good practice to regularly use the “Check for updates” feature to ensure that you have easy access to the most up-to-date information, patches, and tools available. Check out the Security Readiness Kit. It's one more weapon you have at your disposal to fight intrusions. ◆

Because security patches, service packs, guides, and tools are updated regularly, Microsoft designed the SRK to automatically update itself.

WE NEED YOUR FEEDBACK

This issue of *Microsoft Security Watch* is the fourth newsletter we've published this year as a supplement to *Windows & .NET Magazine*. We would like to know your opinion of these newsletters.

It is only in knowing the issues that are of greatest importance to you and your organization that we can hope to improve our security-related content. To let us know your opinion of *Microsoft Security Watch*, please access our survey at the following URL: http://www.winnetmag.com/securitywatch.

The survey shouldn't take more than 15 minutes to complete. Please take time to respond. We thank you in advance for your participation.

Better Together:

ISA Server 2000 and Microsoft Exchange Server

by Thomas W. Shinder

Email is the engine that drives today's business. While most businesses can survive for a day or two without the corporate Web Server, FTP server, or file server, the loss of email access for even one day can often prove to be catastrophic. Even when the mail servers are humming along without fail, lack of access can prove devastating. An innocent day away from the office—and away from the office email—can lead to a lost meeting, a lost lead, and a lost opportunity.

Remote access to Exchange Server services is a powerful weapon against this kind of lost opportunity. No longer does a day away from the office have to mean a day away from business-critical email. Just pull out the trusty PDA, Internet-enabled cell phone, or laptop computer and connect to your office mail—easily and securely. If something important comes up, you can respond right away.

THE CHALLENGE OF SECURE REMOTE ACCESS

You can use any firewall to provide remote access to your email that's stored on a Microsoft Exchange Server located on the internal network. Your challenge is to allow secure remote access to Exchange email services. Secure remote access requires that you configure your firewall to forward inbound connection requests from hosts on the Internet to your Exchange Server on the internal network in a way that allows the greatest level of access combined with the highest level of security.

You can allow inbound access to Exchange Services on the corporate network in several ways. The method that traditional firewalls use is typically referred to as "port forwarding." The firewall accepts an inbound connection request from an email client on the Internet on a predefined IP address and port, and forwards those requests to the Exchange Server on the internal network. For example, let's say an external email client needs to download mail via the POP3 protocol. You configure the firewall to accept incoming connections on TCP port 110 and then forward the connection to TCP port 110 on the internal network's Exchange Server.

The problem with this port forwarding approach is that conventional firewalls do nothing but prevent inbound connection requests to unapproved ports. For approved ports, the firewall just forwards the connection request and passes the packets. The traditional firewall doesn't evaluate the validity of the messages moving between the email client and Exchange Server; it doesn't know how.

MODERN APPLICATION LAYER-AWARE FIREWALLS

Unlike traditional firewalls, modern firewalls use *Application Layer Filtering* methods to examine the Application Layer (or layer 7) contents of the communication. The application layer-aware firewall is able to perform the same type of port forwarding as the conventional firewall, but it is also able to inspect the communications moving between the email client and Exchange Server. In our POP3 example, the application layer-aware firewall can check for valid POP3 commands so that buffer overflow attacks against the internal network's Exchange Server will be thwarted at the firewall.

The day of the conventional firewall is over. TCP/UDP port-based access control is inadequate in today's complex networking services environment. Any port can be used to host any service, and alternate protocols can be used to "wrap" (encapsulate) and "transport" other protocols. An example of this type of encapsulation is the RPC over HTTP protocol that allows Exchange RPC Messages to be wrapped inside an HTTP message to be passed through firewalls.

Another example is the "HTTP tunneling" proxy services. These nefarious applications and service providers let users subvert firewall policies by wrapping unapproved protocols such as NNTP and IRC inside HTTP communications. The traditional firewall, using port-based access control, passes the packets because it's completely unaware of the application layer data contained inside the HTTP communication.

ISA Server 2000 solves the problem of secure remote access to Exchange Services with its sophisticated layer 7 awareness. In fact, ISA Server 2000 could be considered the model of an application-layer firewall because of its progressive access control and connection inspection mechanisms. A properly configured ISA Server 2000 firewall is a powerful method of preventing unauthorized inbound and outgoing access, to and from the internal network. In addition, the properly configured ISA Server 2000 firewall provides a detailed audit trail that lets you perform comprehensive forensic analysis, should that need ever arise.

An ISA Server 2000 firewall protects Exchange servers on your internal network by using several unique features that you won't find on any other firewall in ISA server 2000's class.

An ISA Server 2000 firewall protects Exchange servers on your internal network by using several unique features that you won't find on any other firewall in ISA Server 2000's class:

- Secure remote access for the Outlook MAPI client using ISA Server 2000 secure RPC
- Secure remote access for Outlook Web Access (OWA), Outlook Mobile Access (OMA) and Exchange ActiveSync (EAS) using SSL bridging with delegation of basic authentication
- Secure remote access for the full MAPI Outlook 2003 clients connecting to Exchange 2003 Servers using the RPC over HTTP

Let's look at each of these features in more detail to provide you with a better idea of the high level of security ISA Server firewalls provide, while at the same time enhancing the email experience for your remote workers.

USING SECURE RPC PUBLISHING

Employees who travel must be able to connect to the Exchange server using the same device when they're at the office and when they're on the road. Organizations that have standardized on the full Outlook 2000/2002/2003 MAPI client can use the full array of options and services provided by Exchange. The full MAPI client provides the richest email experience for Outlook users.

The problem is that, when security is important, users have to switch between the full Outlook MAPI client and Outlook Express. They can connect to the Exchange Server and use the full Outlook MAPI client when they connect directly to the corporate network, but when they're on the road, they have to use Outlook Express because traditional firewalls can't be configured to allow secure inbound access for the full MAPI client.

The Microsoft Knowledgebase article "XCCC: Exchange 2000 Windows 2000 Connectivity Through Firewalls" (http://support.microsoft.com/?kbid=280132) describes the static port assignments required to allow inbound access for the full Outlook MAPI client through a traditional firewall. The static packet filters required create an unacceptably insecure firewall configuration because they allow inbound access to core Active Directory related services. In addition, traditional firewalls do not understand the commands passed between the full Outlook MAPI client and the Exchange server and can't assess the validity of these commands.

The solution to this problem is ISA Server 2000 secure Exchange RPC Publishing. Secure Exchange RPC publishing leverages the ISA Server 2000 RPC Application Filter. This Application Filter is able to inspect and manage the communications between the full Outlook MAPI client and the Exchange Server. Only valid connection requests are honored; invalid connection attempts and exploits are dropped.

Another advantage of secure Exchange RPC Publishing is that no static ports need to be opened on the ISA Server 2000 firewall. You create a secure Exchange RPC Server Publishing Rule that allows inbound connection requests from remote Outlook MAPI clients to be forwarded to the Exchange Server on the internal network. Only TCP port 135 is open and only valid Exchange RPC messages are allowed.

ISA Server 2000's secure RPC Publishing provides a unique and rare example of a case where security and functionality are directly related. Security and functionality are typically inversely related: the more secure a solution is, the lower the functionality provided to users. In contrast, secure Exchange RPC publishing provides both a higher level of security and a higher level of functionality.

The best example of the security provided by ISA Server 2000's smart RPC filter is illustrated by the recent worms that exploit issues with the Windows RPC mechanisms. Organizations that allowed remote access for the full Outlook MAPI client via any other firewall were at risk of being infected by the Blaster worm and its variants. No other firewall was able to evaluate the nature of the RPC connection request and those firewalls passed the RPC connection requests directly to the Exchange server without intelligent application layer inspection. The result was that unpatched Exchange Servers were infected with the Blaster worm and suffered downtime and potential data loss because they didn't use a secure ISA Server 2000 firewall.

Organizations that used ISA Server's secure Exchange RPC publishing were protected from external attack. Even Exchange Servers that remained unpatched were immune from external attack by the blaster exploit. And while all servers must be patched, the ISA Server 2000 firewall provided the extra time administrators needed to evaluate the patch and install it on their Exchange Servers.

The Outlook client can be configured to use 56-bit MD5 encryption for its communications with the published Exchange Server. The problem with this setup is that you had to depend on the Outlook client to be configured correctly. If the client was not configured to use encryption, then the messages would traverse in an unencrypted state between the Outlook client and published Exchange Server. The good news is that ISA Server 2000 Feature Pack 1 corrects this problem by allowing to force an encrypted connection between the Outlook client and Secure RPC published Exchange Server.

USING SSL BRIDGING WITH DELEGATION OF BASIC AUTHENTICATION

Remote users often connect from networks that allow only outbound HTTP and SSL connections (for example, from hotels that provide Internet access). This simplifies firewall management for the hotel operators, but can play havoc with a remote access email solution that is based on the full Outlook MAPI client or SMTP/POP3/IMAP4 clients. Fortunately, Outlook Web Access (OWA), Outlook Mobile Access (OMA) and Exchange ActiveSync (EAS) provide a viable subset of features that lets the remote user have a good email experience.

Traditional firewalls are configured to pass incoming HTTP and SSL connections from the firewall's external interface to the OWA server on the internal network. This provides an

ISA SERVER FEATURES AT A GLANCE

Advanced Application-Layer Protection Beyond Traditional Firewalls

Technology	**Capabilities**
Application-layer filtering	Delivers enhanced security and ease of use beyond that of traditional firewalls for e-mail server, Web server, and Microsoft Office Outlook® Web Access deployments. Capabilities include built-in intelligent filtering of HTTP, FTP, Simple Mail Transport Protocol (SMTP), H.323 (a multimedia communication protocol), streaming media, remote procedure calls (RPCs), and more.
E-mail filtering	Enhances e-mail server security through an improved capability to help filter out e-mail that contains unwanted keywords or file attachments.
Exchange RPC filtering	Provides protection for remote Outlook users accessing Exchange Server over untrusted networks without a VPN.
Enhanced security for Outlook Web Access and IIS	Improved authentication and protection from evolving types of Internet attacks enables ISA Server to better secure servers running Internet Information Services (IIS) and Outlook Web Access.
Stateful inspection	Examines data crossing the firewall in the context of its protocol and the state of the connection. Dynamic packet filtering opens ports only when necessary.
Extensible filtering architecture	Extends ISA Server with many partner add-ons that add capabilities such as URL filtering, antivirus, load balancing, and more. Enables you to develop application filters that intercept, analyze, or modify any protocol over any port. You can also create Web filters, based on Internet Server Application Programming Interface (ISAPI), for viewing, analyzing, blocking, redirecting, or modifying HTTP, HTTPS, and FTP traffic.
Bandwidth priorities	Sets bandwidth priorities to optimize resource allocation, prioritizing bandwidth by user, group, application, destination site, or content type.

Fast and Secure Proxy and Cache

Technology	**Capabilities**
High-performance Web proxy and cache	Accelerate users' Web access and save network bandwidth through the fast RAM caching and optimized cache store in ISA Server.
Scalability	Scale up your cache easily and efficiently by adding servers with dynamic network load balancing and the Cache Array Routing Protocol (CARP). Take advantage of multiple processors with the optimized symmetric multiprocessing (SMP) architecture.

Fast and Secure Proxy and Cache continued

Technology	Capabilities
Distributed and hierarchical caching	Configure your network to place caches closest to users or in chained configurations, with multiple and backup routes.
Active caching	Optimize bandwidth usage with proactive and automatic refreshing of popular content.
Scheduled content download	Distribute content and preload the cache on a defined schedule, ensuring efficient use of the network, consistent mirrored servers, and offline availability.
Streaming media support	Transparently support popular media formats and save bandwidth by splitting live media streams on the gateway.

Integrated Acceleration, Access Control, Security, and VPN

Technology	Capabilities
Windows 2000 Server integration	ISA Server users, configuration, and rules work with the Microsoft Windows® 2000 Active Directory® directory service. Authentication, network services, bandwidth control, and management tools extend Windows 2000 Server technologies.
Multilayer firewall	Maximize security with packet-, circuit-, and application-layer traffic screening.
Broad application support	Work with dozens of major Internet applications using predefined protocols including transparent Secure Network Address Translation (SecureNAT), Web proxy clients, Authenex A-Key, RSA SecurID, Active Directory, IIS, OWA, Exchange, Microsoft SQL Server™ 2000, Microsoft BizTalk® Server 2002, and application filters.
Integrated VPN	Provide standards-based, secure site-to-site, and remote access VPN with the integrated services of Windows 2000 Server over the PPTP and L2TP/IPSec protocols.
System hardening	Lock down Windows 2000 Server by setting the appropriate level of security using predefined templates.
Integrated basic intrusion detection	Identify and respond to common network attacks such as port scanning, WinNuke, and Ping of Death using technology licensed from Internet Security Systems (ISS).
Transparency for all clients	Provide extensible, transparent firewall protection for all Internet Protocol (IP) clients using SecureNAT, without the need for client software installation, or deploy Firewall Client and have transparent authentication and broad application support.
Advanced authentication	Enforce strong user authentication with Windows integrated authentication (NTLM and Kerberos), digital certificates, basic mode, and digest mode support using the optional Firewall Client software.

effective remote access solution, but at the cost of abysmal security. More sophisticated firewalls are able to examine the HTTP connections and determine if those connections are valid and drop invalid packets that contain potential exploits.

The problem is that even these more sophisticated firewalls can't evaluate the validity of the commands and data in an SSL connection. The information is hidden inside the SSL stream, which is encrypted between the OWA client and OWA server on the internal network. The only thing the firewall can do is to pass the packets and hope that the OWA server is able to evaluate the validity of the messages itself.

ISA Server 2000 firewalls solve this problem by supporting SSL to SSL bridging. The ISA Server 2000 firewall acts as an SSL "bridge" between the OWA client and OWA server on the internal network. While these SSL packets "cross the ISA bridge," the packets are unencrypted and inspected. Packets that fail inspection are dropped. Inspection can be performed by a special version of URLScan included with ISA Server 2000 Feature Pack 1 (http://www.microsoft.com/downloads/details.aspx?FamilyID=2f92b02c-ac49-44df-af6c-5be084b345f9&DisplayLang=en). You can install third-party applications to further enhance the inspection mechanism.

How does SSL to SSL bridging work? First, the OWA client negotiates an SSL link with the external interface of the ISA Server 2000 firewall and sends the connection request through this link. The ISA Server 2000 firewall decrypts the SSL messages and exposes them to its application layer inspection filters. The ISA Server 2000 firewall drops connections that don't meet its validity requirements.

If the packets are valid, then the ISA Server firewall creates a second secure SSL link. This time, the SSL link is between the ISA Server 2000 firewall's internal interface and the

OWA server on the internal network. Data transferred between the ISA Server firewall and the OWA server on the internal network are passed through this second link.

The OWA server's responses are passed to the ISA Server firewall's internal interface through the second link. The ISA Server firewall again decrypts the messages, examines them for validity, and then e-encrypts the valid messages and forwards them to the remote OWA client via the first SSL link. As you can see, there's a lot of encryption and decryption going on here.

ISA Server 2000 firewalls are unique in that they can inspect the contents of an end-to-end SSL connection. Normally, the contents of an SSL link between the SSL client and SSL server are hidden from the firewall because the firewall is unable to inspect the encrypted data. ISA Server 2000's clever SSL to SSL bridging mechanism solves this problem.

The level of security provided by SSL to SSL bridging can be further enhanced by using the delegation of basic credentials feature provided by ISA Server 2000 Feature Pack 1. You don't need to worry about using basic authentication because the SSL link prevents the credentials from being intercepted. Traditional firewalls pass authentication requests from the OWA client to the OWA server and allow a direct communications link between an unauthenticated client and the OWA server in the process. This is risky because there's a significantly higher chance that an unauthenticated host is an attacker.

ISA Server 2000 firewalls protect the OWA server from this problem by requiring the OWA client to authenticate with the firewall first. The firewall then acts on behalf of the OWA client and forwards the user credentials to the OWA server. Only after the user is successfully authenticated does the ISA Server 2000 firewall allow anything to pass from the OWA client and OWA server.

OWA provides significant improvement over SMTP/POP3/IMAP4 client access, but it still suffers from providing a subset of the full Outlook MAPI client's features. In addition, the OWA interface varies from the full Outlook MAPI client interface and this can be disconcerting for remote users and reduce their overall level of productivity. An ideal solution is to provide the firewall friendliness afforded by OWA and the full, feature-rich email and collaboration experience provided by the full Outlook MAPI client.

USING SECURE RPC OVER HTTP

The ideal solution is here in the form of secure RPC over HTTP connectivity. If you have Outlook 2003 and Exchange Server 2003, you can use the RPC over HTTP protocol to allow remote Outlook MAPI clients access to the Exchange Server. The RPC messages are contained in the HTTP communication and an RPC over HTTP proxy unwraps the messages to expose the RPC commands and forwards them to the Exchange Server.

ISA Server 2000 is able to secure the RPC over HTTP connections in the same way that it secures the OWA connections, by using SSL to SSL bridging and delegation of basic credentials. The connection between the Outlook 2003 client and the external interface is secured by SSL and the connection between the internal interface of the ISA Server 2000 firewall and the RPC over HTTP proxy on the internal network is secured by SSL. The ISA Server 2000 firewall examines the HTTP messages moving between the Outlook 2003 client and RPC over HTTP proxy server on the internal network and drops invalid HTTP connections.

Outlook 2003 RPC over HTTP provides an effective blend of security and accessibility. All links between the Outlook 2003 client and Exchange Server are encrypted and client certificate authentication can be added to the mix to further enhance the level of security. However, the level of security provided by SSL secured RPC over HTTP connections is not as high as that afforded by ISA Sever 2000 Secure Exchange RPC Publishing. The layer 7 aware RPC application filter prevents RPC exploits from reaching the Exchange Server. Connections made over a RPC over HTTP link are not exposed to the RPC filter and could potentially be struck by an RPC exploit. However, only Outlook 2003 clients can use the RPC over HTTP protocol and there have been no reported exploits against this the proxied RPC over HTTP connection.

Remote access to corporate email requires a firewall that can secure the connection between the mail client and the Exchange server. In addition, the user experience should not be degraded because of limitations in the firewall technology that allows inbound connections to the Exchange server. ISA Server 2000 firewalls provide a high level of security by leveraging SSL to SSL bridging, basic authentication, forced encryption for MAPI client connections, HTTP protocol inspection, and RPC over HTTP. The intelligent layer 7-aware ISA Server 2000 firewall gives remote users the best possible email experience with a higher level of security for the connection than any other firewall in its class. It just doesn't get much better than that. ◆

Thomas W. Shinder, MCSE, is a computing industry veteran who's worked as a trainer, writer, and consultant for Fortune 500 companies, including FINA Oil, Lucent Technologies, and Sealand Container Corporation. Tom was a Series Editor of the Syngress Windows 2003 Certification Study Guides and author of the books *Configuring ISA Server 2000: Building Firewalls with Windows 2000* and *ISA Server and Beyond*. Tom is the editor of the Sunbelt Software WnXPnews newsletter, a regular contributor to TechProGuild, and content editor, contributor and moderator for a leading site on ISA Server 2000, www.isaserver.org.

ADVERTISER-SPONSORED CASE STUDY

Utility Engineering Enhances ISA Server Capabilities with Solutions from Burst Technology

Phillip Jones discovered just how two-edged a sword Internet access could be when his employer, Utility Engineering Corporation, mandated that Internet access be provided to all its more than 600 employees. Utility Engineering is a service firm for the power generation industry and a wholly owned subsidiary of Xcel Energy. At the behest of their parent, Utility Engineering, a Microsoft Windows 2000 server shop, was implementing a corporate-wide policy to provide Internet access so that its employees could obtain their health and benefit information online.

Jones, the general manager of Information Systems, quickly found that the new policy, instituted for the benefit of Utility Engineering employees, had a downside—for both the corporation and workers. Bandwidth shortages appeared as employees began using the Web for non-business use, such as listening to online radio broadcasts and downloading MP3's. And more disturbingly, it became apparent that some workers were visiting Web sites that violated Utility Engineering's acceptable use policy—and could land the company in legal troubles.

FINDING THE RIGHT TOOL

Jones realized that while monitoring Web usage was always a necessity, he needed an easier way to do it enterprise wide. He purchased a software tool that would let him determine how employees were using Internet access across four locations throughout the U.S. The tool Jones chose worked adequately, but he found that generating reports was both time-consuming and burdensome. The tool originally installed required software implementations on each of his ISA servers. Complicating the situation was the fact that the tool required separate reports to be created for each server—there was no way to generate a single report across the network.

Enter Burst Technology, a Florida-based software developer that focuses on solutions for Web, email, and log analysis solutions for Microsoft environments. Burst's bt-LogAnalyzer offered Jones something that went beyond adequate: it allowed him to generate a single report that covered all of his remote Microsoft ISA servers, thus putting an end to the administrative headache that went with having to manage four remote servers. In addition, Jones found that Burst's product also allowed him to analyze Exchange logs for emails.

Jones, a 21-year employee of Utility Engineering and its previous parent company, realized from the results of bt-LogAnalyzer that "good employees can sometimes do really stupid things"—like going to Web sites that violated the company's Internet use policy and potentially exposed Utility Engineering to legal liability, not to mention being in places you shouldn't go on company time. He turned once again to Burst Technology, which offered a second piece of the solution: bt-WebFilter. bt-WebFilter gave him the ability to record the places employees were surfing and block access to sites that could create bandwidth and liability issues. Many times, according to Jones, just showing an employee a monitoring report of their Internet-related activities is enough to correct problems.

AN APPEALING SOLUTION

Two things especially appeal to Jones. First, bt-WebFilter allows easy replication across the network, which means that all his remote Microsoft ISA servers can be updated daily, with URLs added or deleted as necessary. Second, bt-LogAnalyzer has opened Jones's eyes to the amount of spyware that had previously been getting downloaded onto employee machines. "That was a real revelation," he said. "You just have no idea what's being installed on people's computers without anyone's knowledge until you have a tool to block things from getting in. It's really amazing…and scary."

With bt-WebFilter and bt-LogAnalyzer, Jones discovered that he could shield the company from legal liability—while protecting employees from occasional lapses. Importantly, bt-LogAnalyzer is the only product that can make a distinction between sites that an employee clicks on and sites that were pushed to their desktop by pop-ups.

Phil's final word on Burst Technology's products: "They're doing a great job in my Microsoft environment by providing us with the ability to enforce policies and better protect our enterprise."

BURSTechnology

Burst Technology
239-495-5900
www.burstek.com

GFI DownloadSecurity Protects Manufacturer Against Malicious Downloads

Chris Moss, accounting and IT manager at THERMO-KOOL/ Mid-South Industries, selected GFI DownloadSecurity for ISA Server to protect his system against viruses, Trojans, and malicious content in downloaded files. THERMO-KOOL, with more than 100 employees, is a leading U.S. manufacturer of custom walk-in refrigeration and freezers. GFI Download-Security is a content security product that controls what files enter the network via FTP and HTTP and ensures that they are virus free and not malicious.

As part of his research to step up the organization's network security, Moss came across GFI's online Security Testing Zone (http://www.gfi.com/emailsecuritytest/) where he ran the site's free security tests to determine how well-protected his network really was against viruses, worms, and other malicious content. "I evaluated GFI's email virus tests and was impressed with the added functionality that content checking could offer in providing protection against harmful content," he said.

THE RISK OF INFECTED DOWNLOADS

THERMO-KOOL identified the need for a product to provide content checking and anti-virus protection for downloads. This product had to integrate with ISA Server 2000 because the THERMO-KOOL had recently acquired ISA Server as an upgrade from Proxy Server 2.0.

"Microsoft ISA Server gave us the ability to integrate with Active Directory, which enables us to limit Internet access by groups," Moss explained. "Also, ISA Server is much more extensible. We can add additional plug-ins to provide content checking and other features."

THERMO-KOOL was pleased to be able to try a full version of GFI DownloadSecurity before purchase. "Access to evaluation products was really important to us and we were delighted that GFI allows potential customers to download a free, full-trial version for a month or two," Moss said.

PROTECTING AGAINST MALICIOUS FILES

GFI DownloadSecurity for ISA Server handles the security risk of file downloads without resorting to blocking all file downloads at the firewall level. Instead, it content checks downloaded files and can quarantine them based on file type and user. Its core security features include:

- Multiple virus engines, to guarantee higher detection rate and faster response to new viruses
- Content checking, to quarantine dangerous files and content
- Blocking and quarantining of files based on file type and extension
- Checking and blocking applications' hidden downloads
- Trojan and executable scanner, to detect malicious executables
- Network-wide blocking of Java applets and ActiveX controls.

"We were impressed by GFI DownloadSecurity and preferred its features over those of other products. The inclusion of multiple virus engines, content rules, and scanning before items were saved on the network were huge plus points," Moss said. "Also, the fact that the files were checked during downloads was crucial to us."

GFI DownloadSecurity was built from the ground up to work with ISA Server. It links in as an ISAPI extension and can leverage features such as alerts and reporting that are already found in ISA Server—without necessitating any changes to the organization's network configuration. Its use requires no learning curve on the part of the users.

A COST-EFFECTIVE SOLUTION

Users do not notice GFI DownloadSecurity until they download a file. Then GFI DownloadSecurity displays a download progress dialog box and the download proceeds. Once the download is complete, GFI DownloadSecurity scans the file for viruses. If the file has no viruses and does not trigger a rule, the user receives it immediately. If the file triggers a rule, it is put into quarantine for administrator approval. Once approved, the file is sent to the user as an email attachment or link. If the file is rejected, the user is notified.

Describing the product's key benefits, Moss remarked: "GFI DownloadSecurity is cost-effective because it enables us to license by authorized Internet user, rather than by the entire Active Directory user list. Also, GFI DownloadSecurity provides us with a front-line defense against threats at the firewall, giving a multiple-layer defense against attacks and malicious content."

GFI

GFI Software Ltd.
www.gfi.com

ADVERTISER-SPONSORED CASE STUDY

Fresno County Uses Microsoft Security Solution to Protect Consolidated Network Portal

To meet increased demand from internal users and the public for Web-based services, California's Fresno County upgraded its network security solution from Microsoft Proxy Server to Microsoft Internet Security and Acceleration (ISA) Server 2000. ISA Server provides Fresno County with a high level of security, improves bandwidth by 50 percent, and simplifies day-to-day network management. Seamless integration with Windows 2000 technology lets ISA Server provide the county with an economical, scalable, and secure infrastructure that positions the county for future growth.

THE SITUATION

Fresno County prides itself on being one of the most technologically advanced county governments in California. The solution it had designed in the early 1990s, however, had grown to include 15 Proxy Server–based systems and six Web servers running Internet Information Services (or IIS, the Web server built into Windows 2000 Server) connected to the county's internal network and the Internet. This solution included more than 20 portals that needed protection against attack, and increasing user demand for online services created even more complexity. The county needed a secure, reliable, and scalable solution that would let it consolidate IIS, FTP, and other Internet services in one secure location.

Budget considerations mandate that Fresno County leverage its current infrastructure while creating more opportunities to increase Internet and extranet services. "We anticipate a huge demand for Internet services from employees and the public," says Ron Talent, division manager of network and server administration. "We needed a more secure network that will give us room to grow, and we chose Microsoft technology to get us there."

THE SOLUTION

Fresno County has approximately 350 Windows-based servers, 40 IBM AIX UNIX-based servers, and 500 Cisco network devices. The county's IT equipment is in several locations, but the Network and Server Administration division manages it all from a central technology center. The county has approximately 8,000 desktop computers, all standardized on Windows 2000 Professional and Microsoft Office. Talent describes the county as "primarily a Dell shop," with various models of Dell hardware that are being upgraded.

To protect its network, Fresno County has a two-tier firewall solution. All access to the county's Internet connection comes first into a Cisco PIX firewall for basic packet filtering and monitoring of connection status. Behind the PIX firewall are two pairs of machines running Windows 2000 Server and ISA Server.

Rather than follow a traditional network design, Fresno County's network forwards traffic to one of two pairs of ISA Server–based machines directly behind the PIX firewall. Where traffic is forwarded depends on the kind of access required: All network services that permit anonymous access are behind one pair of ISA Server firewalls; all network services that require user authentication are behind the other pair. Besides protecting publicly available information that requires user authentication, the second pair also protects the county's internal network.

Additionally, Active Directory is installed behind the second pair to provide centralized network security, while allowing the IT staff to manage and share information about resources and users.

HIGHER LEVEL OF SECURITY

Although unusual, this network design works well for Fresno County. "Having all of our applications that need extra security on the same network has simplified our overall network design," says Eric Eidness, senior network systems engineer. "And the level of security is high, because access to those resources requires authentication and users have to pass through two firewalls. The Cisco PIX routes information and users to the appropriate set of ISA Server machines, based on whether the user is seeking information that is 'open access' or requires authentication." The deep content inspection enabled by ISA Server's application-layer filtering capability helps ensure that only legitimate traffic is allowed into both networks.

Microsoft®

Microsoft
http://www.microsoft.com/isaserver

NetIQ's Marshal Helps Law Firm Secure Electronic Content

Arnall Golden Gregory LLP (AGG), headquartered in Atlanta, is a mid-size law firm that provides innovative legal counsel to entrepreneurial and growing companies in a number of industries. With more than 350 employees, AGG counsels clients across a broad range of industries, including biotechnology, e-commerce, food and drug, healthcare, real estate, telecommunications and venture capital.

AGG's Information Services department supports more than 350 employees at two sites. Due to confidentiality issues inherent to their business, they maintain a very tightly controlled environment. The Microsoft Exchange infrastructure at AGG runs on a high availability, redundant server.

GETTING A HANDLE ON SPAM AND EMPLOYEE WEB USAGE

As AGG has grown and become increasingly dependent upon email for business communications—both internally and externally—the amount of spam that AGG received became more of a problem. "We wanted to kill spam. We were just inundated with ridiculous amounts of it," said Paul Grulke, director of information services at AGG. "We had no data on how much we were receiving. There was really no way to tell."

Users were accustomed to using their business email address as their personal email address, adding to the amount of spam AGG received. The firm also had unique requirements based upon the nature of their work. They determined that they would be unable to blanket block spam based upon message content filters because certain words that would typically be flagged could be relevant for communications with certain types of clients—such as healthcare and food and drug—or in litigation. They needed an open, flexible way to block spam.

In addition to combating spam, the firm's management also issued a directive to get control of non-business Web surfing. With users extensively surfing the Web during work hours, employee productivity suffered. By visiting inappropriate Web sites, employees also put the firm at risk of legal liability and the spread of inappropriate material in the workplace. AGG needed a way to grant role-based full and limited Internet access, monitor employee surfing and report on visits to Web sites considered dangerous.

NETIQ MARSHAL SOLUTIONS FIT THE BILL

To get a handle on AGG's spam and Web surfing, Grulke began searching for a monitoring tool that could address these issues. After extensively testing a number of solutions and a recommendation by its business partner Intellinet, AGG picked NetIQ's Marshal family of content security products because they best met the firm's top decision criteria of cost, ease of use, and speed to implement.

"We could not afford to spend the time, money, and personnel resource on something that required a lot of input," Grulke said. "I don't have to manage Marshal. I set it and forget it." While expecting his deployment to take a week, he was pleasantly surprised to discover that the implementation was complete in two days. Grulke liked the rules-based focus of the products and how the rule set tells the user exactly what it is doing in plain, understandable text that is built interactively.

Grulke found the simple interface to be very straightforward and flexible. AGG has implemented role- and rule-based blocking of spam and granting Internet access, setting strict and permissive rules that are applied to an employee depending upon their role in the organization. "I'm really only limited by me and my creativity as to how I'm going to handle the message," he said.

A CHANGED ENVIRONMENT

Since implementing NetIQ MailMarshal and NetIQ WebMarshal, AGG has achieved impressive results. "We now block 5,000 spam messages per day," Grulke said, "with only an average false block of two messages per month." With NetIQ Marshal content security solutions, the firm has taken control of spam and achieved high Exchange availability. NetIQ MailMarshal and NetIQ WebMarshal helped AGG achieve its desired results—reduced costs, improved employee productivity and l imited legal liability due to inappropriate Web surfing.

ADVERTISER-SPONSORED CASE STUDY

CyBlock Web Filter Provides Total Web-Use Management Solution

Maybe it's no coincidence Cottingham & Butler's headquarters is located in Dubuque, Iowa's landmark Security Building—security is a top priority at the 117-year-old firm. Since 1887, Cottingham & Butler has earned a reputation as one of the Heartland's foremost commercial insurance brokerage firms. With a dynamic and innovative management approach, the firm has successfully adapted new technologies to offer the highest level of service and quality to its customers.

From online client services to state-of-the-art systems for insurance brokerage, property and casualty claims, employee benefits claims and coordinated care, Cottingham & Butler relies upon information technology to provide customers with faster, more efficient professional service.

CyBlock Web Filter from Wavecrest Computing helps them do it.

THE CHALLENGE: MANAGING INTERNET ACCESS

Network security, performance and stability are critical at Cottingham & Butler—and with the majority of the company's clients located outside the Dubuque area throughout the continental United States, Internet access is "indispensable" in day-to-day operations, said Database Administrator/Network Administrator Phil Niles.

Like many companies, Cottingham & Butler faced the challenge of providing Internet access for its employees without compromising network security or workforce productivity. As a company specializing in risk management, they took a pro-active approach to Web-use management.

First, they implemented an Acceptable Use Policy (AUP) designed to prevent inappropriate use of the Internet in the workplace, yet allow employees flexible Internet access for business use. It's a policy that reinforces Cottingham & Butler's corporate values: 1) have the interests of your company at heart; 2) act with integrity; 3) tell the truth; 4) keep commitments; 5) treat people with dignity and respect; and 6) promote positive relationships.

"We needed a better idea of how people were using the Internet," Niles recalled. "We were moving over to ISA Server and were looking at reporting capabilities that would help us better manage Internet use."

After migrating to Microsoft's ISA Server 2000 last year, Niles began looking for an Internet filtering and monitoring solution that would help ensure compliance with the policy and manage Internet usage for the firm's 300+ employees.

Niles needed software that would integrate easily with ISA Server 2000 while providing clear, accurate, and customizable user activity reports on large volumes of data. Cottingham & Butler has doubled in size every three to four years for the past 20 years—increasing the need for a solution that was flexible, robust and scalable enough to grow with their company.

The solution was CyBlock Web Filter from Wavecrest Computing.

THE SOLUTION: CYBLOCK FOR ISA SERVER

CyBlock provided Cottingham & Butler with a total Web-use management solution that could do more than simply block access to "obvious legal liability sites." It was CyBlock's combination of flexible blocking and advanced reporting features that set it apart from the competition.

With CyBlock installed on ISA Server, Niles can now efficiently manage Internet usage—automatically blocking access in accordance with Cottingham & Butler's AUP, and generating comprehensive reports on large volumes of data quickly and easily.

"We store about 45 days of log files—that's 50 MB of data each day," Niles said, adding that before CyBlock, "it was impossible to create these types of reports."

Management can now review User Audit Summary and User Audit Detail reports on a regular basis. Reports can be scheduled to run automatically or can be generated ad-hoc whenever needed. In addition to CyBlock's 55 standard categories, Niles uses CyBlock's Custom Category feature (administrators can define up to 12 custom categories), tailoring the software to match Cottingham & Butler's specific needs.

CyBlock's clear, comprehensive reports allow management to spot potentially harmful Internet activity before problems arise—minimizing legal liability, controlling bandwidth costs and protecting the corporate network from security risks.

Together, CyBlock and ISA Server are helping one of the nation's leading commercial insurance providers do what it does best—manage risk.

WAVECREST
COMPUTING

Wavecrest Computing
321-953-5351
877-442-9346 (toll-free)
www.wavecrest.net
info@wavecrest.net

Websense Enterprise: The Right Prescription for E-Enabled Hospital

Frimley Park Hospital is a 700-bed Healthcare Trust institution in Frimley, England serving a catchment population of 365,000 and employing more than 3,500. As well as being the largest hospital in southeast England (according to the percentage of the population it serves), it is also one of the most technically advanced. Frimley Park has continued to meet the stringent targets set by the UK government and was one of the first hospitals to adopt Internet technology within a healthcare environment. Richard Storey, Head of IT at Frimley Park, explains, "All hospitals in Britain are obliged to offer Internet facilities to staff this year. As you can imagine, it is absolutely essential that we have a secure and easily manageable system with which to provide this."

ENSURING ACCESS, ELIMINATING MISUSE

The ability to store patient data online and provide staff with access to the Internet allows the hospital to provide better health care to patients. However, it also brings unwelcome risks. Potential security breaches, Web-based viruses, and enabling users to access inappropriate or illegal content are just a few of these risks. Storey wanted to ensure that providing online facilities did not compromise patient confidentiality or lead to misuse of the systems. He continues, "The hospital is running 24-hours a day, with a constant stream of patients and staff. The potential for Internet misuse in this kind of environment is considerable."

Staff and patients alike are able to access Internet facilities at Frimley Park. These groups have very different needs. "Obviously, the Internet is a valuable source of information for our clinical staff," explains Storey. "Providing instant access to the latest scientific research and data is critical. As patients can also use the system, we need to ensure that only appropriate content is accessible. Websense provided an ideal solution and the implementation was seamless."

Another Internet-related initiative that Storey is in the process of completing is the Patric Centre—a resource for patients who, with the help of volunteers, want to search the Internet for information relating to their condition. He explains, "This is an ideal example of how the Internet can be both a business tool and a support mechanism for patients."

Websense Enterprise allows the hospital to set various parameters to govern Web access according to the individual needs of the user. Previously, objectionable Web sites were blocked manually by the firewall, but this solution proved too inflexible. "Managing staff Internet access using the firewall caused immense restrictions. For example, we run a urology clinic here, and the staff needed to gather information via the Internet, inevitably using certain biological terms in their searches. The firewall put a blanket block on such access. The Websense solution is much more intelligent—we can still block dubious sites, while permitting access to legitimate ones, which means clinicians are ensured the level of access they need." Updates to the list of permitted Web sites can be made at the touch of a button. Storey continues, "We can grant access to a Web site immediately if it is appropriate. This means that as an IT department we are very responsive to the needs of the user."

Websense Enterprise provides employees with time-based quotas, which limit non-work-related use of the Internet to an hour per day for staff. Outside working hours, employees have unlimited access to the Internet via terminals provided in Frimley Park's coffee shop. "As a cost-effective tool for supporting our staff and improving their working lives, the flexibility offered by the Websense solution has been an enormous benefit for us," Storey said.

SECURITY, RELIABILITY, AND VALUE

Frimley Park also deployed Websense Premium Groups' enhanced Internet management capabilities, which run as part of the Enterprise solution. By doing so, it has added an additional layer of security that ensures outside parties are unable to access the network via peer-to-peer applications or spyware, eliminating disruption caused by malicious mobile code, viruses, or Web-based worms.

Storey is pleased with his choice of supplier, explaining, "We select our suppliers extremely carefully and there is good reason for that: We are not spending shareholders' money, we are spending public money. I have to be 100 percent convinced that I will get the best value for the money from any IT solution I implement. I like to be able to install products quickly and see a tangible benefit immediately. Websense delivered that for me."

WEBSENSE®

Websense, Inc.
800-723-1166
sales@websense.com
www.websense.com

Microsoft Partners

TECHNOLOGY PARTNERS

8e6 Technologies
Orange, CA
www.8e6technologies.com/isaserver

ACP
Birmingham, AL
www.acp-inc.com/isaserver

Aelita Software
Powell, OH
www.aelita.com/isaserver

AEP
Boston, MA
www.aep.ie/isaserver

Akonix
San Deigo, CA
www.akonix.com/isaserver

Aladdin Knowledge Systems
Arlington Heights, IL
www.ealaddin.com/isaserver

Aspelle
Boston, MA
www.aspelle.com/isaserver

Authenex
Oakland, CA
www.authenex.com/isaserver

Bindview
Houston, TX
www.bindview.com

Burst Technology
Bonita Springs, FL
www.burstek.com/isaserver

Castify Networks
Alexandria, VA
www.castify.net/isaserver

Certeon
Waltham, MA
www.certeon.com/isaserver

Chutney Technologies
Atlanta, GA
www.chutneytech.com/ISAserver/

Cobion
Kassel, Germany
www.cobion.com/isaserver

CornerPost Software
Duffield, VA
www.cornerpostsw.com/isaserver

F5 Networks
Seattle, WA
www.f5.com/isaserver

Finjan Software
Los Gatos, CA
www.finjan.com/isaserver

GFI Software
Cary, NC
www.gfi.com/isaserver

Intellitactics
Bethesda, MD
www.intellitactics.com/isaserver

FutureSoft
Houston, TX
www.futuresoft.com/isaserver

ITWorx
Burlington, MA
www.fileway.com/ISAServer.htm

Internet Security Systems
Atlanta, GA
www.iss.net/isaserver

N2H2
Seattle, WA
www.n2h2.com/isaserver

nCipher
Woburn, MA
www.ncipher.com/isaserver

NetIQ
San Jose, CA
www.netiq.com

Network Associates
Santa Clara, CA
www.nai.com

Nexus Technology
United Kingdom
www.webconsent.net/isaserver

Oblix
Cupertino, CA
www.oblix.com

OpenNetwork
Clearwater, FL
www.opennetwork.com

Panda Software
Buenos Aires, Spain
www.pandasoftware.com/isaserver

PatchLink Corporation
Scottsdale, AZ
www.patchlink.com/isaserver

Radware
Mahwah, NJ
www.radware.com/ISAServer

Rainbow
Irvine, WA
www.rainbow.com/isaserver

Rainfinity
San Jose, CA
www.rainfinity.com/isaserver

RSA Security
Bedford, MA
www.rsasecurity.com/isaserver

Sane Solutions
North Kingstown, RI
www.sane.com/isaserver

Secure Computing Corporation
San Jose, CA
www.securecomputing.com/isaserver

Stonesoft
Atlanta, GA
www.stonesoft.com/isaserver

SurfControl

Scotts Valley, CA
www.surfcontrol.com/isaserver

Symantec

Cupertino, CA
www.symantec.com/isaserver

Trendmicro

Cupertino, CA
www.trendmicro.com

Venation

United Kingdom
www.venation.com/isaserver

Wavecrest Computing

Melbourne, FL
sales@wavecrest.net
www.wavecrest.net/isaserver

Websense

San Diego, CA
www.websense.com/isaserver

WebSpy

Kirkland, WA
sales@webspy.com
www.webspy.com/isaserver

GLOBAL DELIVERY PARTNERS

Accenture

Chicago, IL
www.accenture.com

Avanade

Seattle, WA
www.avanade.com

Ernst and Young

Boston, MA
http://ey.com/security

HP

Boston, MA
www.hp.com/hps/tech/security/

IBM

San Jose, CA
www-1.ibm.com/services/its/us/isa
_server.html

PricewaterhouseCoopers LLP

New York, NY
www.pwcglobal.com/security

Schlumberger SEMA

Houston, TX
www.slb.com

Unisys

Boston, MA
www.unisys.com/security

REGIONAL DELIVERY PARTNERS

Canada

CMS Consulting Inc.

Toronto
www.cms.ca/isaserver/

Codefusion Communications Inc.

Toronto
www.codefusion.com/isaserver/

CyberSecure, Inc. Rothesay

www.cybersecure.ca/isaserver/

LegendCorp

Toronto
www.legendcorp.com/isaserver/

U.S.

ACP

Birmingham, AL
www.acp-inc.com/isaserver/

Convergent Computing

Oakland, CA
www.cco.com/isaserver.htm

EYT

Chantilly, VA
www.eyt.com/isaserver

Netivity Solutions

Waltham, MA
www.netivitysolutions.com/isaserver/

Quilogy

St. Charles. MO
www.quilogy.com/isaserver

RDA

Atlanta, GA
www.rdacorp.com/ISAServer/

Corbett Technologies

Alexandria, VA
www.corbett-tech.com/isaserver/

Extreme Logic

Atlanta, GA
www.extremelogic.com/isaserver

Guardent, Inc.

Providence, RI
www.guardent.com/isaserver

InDepth Technology

Dublin, OH
www.indepthtech.com/isaserver/

SECURITY RESELLERS

CDW

Vernon Hills, IL
www.cdw.com/isaserver

Insight

Tempe, AZ
www.insight.com/isaserver

Zones, Inc.

Renton, WA
www.zones.com/isaserver